

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. **1:22-MJ-00186**

MULTIPLE DEVICES CURRENTLY LOCATED AT THE
FBI FIELD OFFICE, 2012 RONALD REAGAN DRIVE,
CINCINNATI, OHIO 45236

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252	Certain Activities relating to material involving the sexual exploitation of minors

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Jonathan P. R. Jones, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

FaceTime Video (specify reliable electronic means).

Date: **Mar 31, 2022**

City and state: Cincinnati, Ohio

Stephanie K. Bowman

Judge's signature

Stephanie K. Bowman, United States Magistrate Judge

Printed name and title



ATTACHMENT A

The property to be searched is an Apple iPhone cell phone, with a Purple/Blue Otterbox brand case and a Nook brand tablet with a black case, hereinafter the “Devices.” The Devices are currently located at the FBI Field Office at 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 2252 including:

- a. Any visual depictions of minors engaging in sexually explicit conduct, to include any information associated with such visual depictions such as, but not limited to, creation date, location created, camera/device used;
- b. Any visual depictions of minors, to include any information associated with such visual depictions such as, but not limited to, creation date, location created, camera/device used;
- c. Any communications, in any format, with minors or concerning minors or suggesting a sexual interest in minors;
- d. Any records or information identifying a minor or showing a minor's whereabouts;
- e. Any records or information concerning child pornography, the receipt or distribution of child pornography, or the attempted acquisition of child pornography to include any internet history;

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history; of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or

electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION - CINCINNATI

IN THE MATTER OF THE SEARCH OF
MULTIPLE DEVICES CURRENTLY
LOCATED AT THE FBI FIELD OFFICE,
2012 RONALD REAGAN DRIVE,
CINCINNATI, OHIO 45236

Case No. 1:22-MJ-00186

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jonathan P. R. Jones, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices, as described in Attachment A (the “Devices”)—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation. I entered on duty as a special agent in 2007 and am currently assigned to the violent crime squad of the Cincinnati Division. In this capacity, I investigate matters involving crimes against children, human trafficking, criminal enterprises, and other violent crimes. Prior to Cincinnati, I was assigned to the Toledo Resident Agency and the Lima Resident Agency of the Cleveland Division, where I was assigned a wide array of criminal and national security matters. During my tenure as a law enforcement officer, I have investigated a range of state and federal criminal violations, including those involving white-collar crime, violent crime, drug trafficking, crimes against

children matters, and national security investigations. Since 2006, I have received training and have experience in interviewing and interrogation techniques, arrest procedures, search and seizure, search warrant applications, and various other crimes and investigation techniques, to include several Title III investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPhone cell phone, with a Purple/Blue Otterbox brand case and a Nook brand tablet with a black case, hereinafter the “Devices.” The Devices are currently located at the FBI Field Office at 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236. The property is particularly described in Attachment A.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

APPLICABLE STATUTES

6. Title 18, United States Code § 2252, generally prohibits the transportation or shipping in interstate commerce the visual depictions of a minor engaging in sexually explicit

conduct. It also prohibits the receipt, distribution, access with intent to view, and possession of such visual depictions when involved in interstate or foreign commerce.

PROBABLE CAUSE

7. On 03/21/2022, FBI Task Force Officer Jacob Popp, with the Ohio Adult Parole Authority (OAPA), contacted your affiant advising of the 03/17/2022 arrest of Johnathan Michael Evans (DOB XX/XX/1975), at his residence, by OAPA after Evans admitted to viewing child pornography. Popp advised Evans was a registered sex offender under OAPA supervision. TFO Popp provided a copy of the report detailing Evans's arrest. The report contained the following narrative:

8. Adult Parole Officers William Hall, John Eckman, and Samantha Chamberlain were conducting field work in the city of Middletown, Ohio, Warren County. Officers came into contact with a Jonathan Evans at 5675 Stone Path Drive Middletown, Ohio. Evans is an offender under supervision with the State of Ohio for a sex offense out of the State of Texas. As part of his parole conditions; he is to have no unsupervised contact with minors, not permitted to view or possess pornographic material or patronize sexually oriented business. During conversation with the offender, he admitted to Officer Chamberlain and Officer Eckman that he had been struggling with abstaining from pornography. When asked what type of pornography he has been viewing, he stated that he views videos containing adults but also children. He identified that he often goes to websites that are frequented on the "dark web", sites such as inxx.in or other sites that are known to have child pornography. At this time, officers reviewed his phone and search history along with images, not finding accessible material. He stated that he does delete material after viewing. His cell phone (352-231-0557) was confiscated, as well as a tablet that he has

ownership of. Offender was taken into custody and transported to the Warren County Jail. The offender discussed his underlying offense; that his victim was his 6-year old niece. At this time, offender remains in custody of the Warren County Jail on an APA hold, pending further investigation. A report will be sent to the state of Texas to notify of the violations.

9. On 03/24/2022, your affiant retrieved the above referenced Devices from TFO Popp in anticipation of obtaining a search warrant. TFO Popp advised Evans advised the PIN code for his iPhone was 426855. At the time of collection, it was noted by your affiant that the Apple cell phone was powered on, but in “Airplane Mode¹”, while the Nook tablet was powered off.

10. A criminal history check identified Evans as a registered sex offender. Evans was arrested 07/18/2021 by the Fort Bend County Sheriff’s Office in Texas and charged with a second degree felony of “Indecency With A Child Sexual Contact”. The victim was ten years old. The criminal history indicated Evans’s was convicted via plea on 10/06/2021 and given a deferred sentence with ten years probation.

11. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

¹ Airplane Mode is a device configuration that permits users to disable a devices’s ability to connect to cellular or WiFi networks or to Bluetooth. At the time of collection, Evan’s cell was configured so that cellular and WiFi network connection were disabled but Bluetooth connection was enabled.

**CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT,
RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY**

12. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of

children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence or inside the collector’s vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of

individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, Internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

g. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

13. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

14. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a

removable memory card in the camera. These memory cards often store up to 64 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer. Additionally, almost all cell phones today can record high-resolution photographs and videos.

15. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

16. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs,

DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera or a cell phone, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person.

17. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

18. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.

19. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user’s Internet activities generally

leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. In my training and experience, examining data stored on the Devices can uncover, among other things, evidence that reveals or suggests who possessed or used the device and where.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

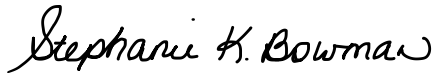
27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Jonathan P.R. Jones
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 31 day of March, 2022
via electronic means, specifically Facetime video.



THE HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an Apple iPhone cell phone, with a Purple/Blue Otterbox brand case and a Nook brand tablet with a black case, hereinafter the “Devices.” The Devices are currently located at the FBI Field Office at 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 2252 including:
 - a. Any visual depictions of minors engaging in sexually explicit conduct, to include any information associated with such visual depictions such as, but not limited to, creation date, location created, camera/device used;
 - b. Any visual depictions of minors, to include any information associated with such visual depictions such as, but not limited to, creation date, location created, camera/device used;
 - c. Any communications, in any format, with minors or concerning minors or suggesting a sexual interest in minors;
 - d. Any records or information identifying a minor or showing a minor's whereabouts;
 - e. Any records or information concerning child pornography, the receipt or distribution of child pornography, or the attempted acquisition of child pornography to include any internet history;
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history; of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or

electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.